REMARKS

The examiner rejected Claims 1, 7, 11, 12-14, 14-1 7, 22, 24, and 29 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The examiner argued regarding claims 1, 7, 11, 24 and 29:

> **With regards to claim 1, 7, 11, 24, and 29, the cited claims define a device that examines traffic "as if the device was disposed on links that are downstream from links that the provisioned monitor is disposed on." Examiner in unclear as to what property this limitation instills upon the device. Further, Examiner can ascertain no structural elements either explicitly or implicitly from this limitation.**

Applicants' claims 1, 7, 11, 24 and 29 particularly point out and distinctly claim the subject matter of what Applicants consider to be their invention.

Applicants have amended claim 1 to call for a device, coupled to physical links between the data center a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links and collects statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

Applicants describe that:

> The provisioned monitor, e.g., gateway 26 logically analyzes traffic on a link or links so as to provide monitoring capabilities for hosted customers C_i equivalent to what could be obtained by placing physical monitors on those hosted customers' individual access links. The provisioned gateway 26 provides monitoring capabilities for many smaller links in the data center by analyzing traffic on a larger upstream link.
>
> Referring now to FIG. 2, the data center 20 has a plurality of links 21a-21n with the Internet 14. Each customer Ci (0 <= i < N, for N customers) of the data center is associated with a set of addresses Ai. The provisioned monitor has a notion of inbound and outbound packets, obtained directly from the physical link's transmit and receive ports. Any inbound

```
packet with a destination address in Ai is
interpreted as inbound to customer Ci.  Every
outbound packet with a source address of Ai is
interpreted as outbound from customer Ci.  Inbound or
outbound packets with other addresses (e.g.,
addresses that are not in the address space Ai for
any customer i) are classified as "other".  Inbound
packets with unknown destination addresses may be
destined to customers that have not been provisioned.
Outbound packets with unknown source addresses may be
coming from customers that have not been provisioned,
or they may be part of a spoofing attack.
```

One of ordinary skill in the art would appreciate the metes and bounds of this invention, in that claim 1 clearly calls for the structural elements of a device, coupled to physical links between the data center a network. The device is configured so that the device examines traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between the network and the data center .... Claim 1 requires a device that collects statistical information over the coupled physical links for a plurality of customers and examines traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

As expressed above, the device as a provisioned monitor has a notion of inbound and outbound packets obtained from the physical link's transmit and receive ports and by examination of source and destination addresses. Thus, one of ordinary skill in the art would understand that "as if the device was disposed on links that are downstream from links that the provisioned monitor is disposed on." refers to an arrangement in which a device at the data center collects packet information at links into the data center for various provisioned customers located on downstream links, e.g., customers' individual access links.

Applicant has amended claim 11 to call for a provisioned monitor, placed on selected links in the data center so that the provisioned examines traffic entering or leaving that data center on the selected links and that collects statistical information for a plurality of provisioned customers, which are on links that are downstream from the selected links that the provisioned monitor is disposed on, the provisioned monitor maintaining separate counter logs for each provisioned customer.

One of ordinary skill in the art would understand claim 11 to encompass an arrangement in which a provisioned monitor is placed on selected links in the data center and examines traffic entering or leaving the data center on the selected links. The provisioned monitor collects statistical information for the traffic from provisioned customers that are on downstream links from the selected links that the provisioned monitor is disposed on. Thus the arrangement would encompass a provisioned monitor having a notion of inbound and outbound packets, obtained directly from the physical link's transmit and receive ports and by examining source and destination addresses. One of ordinary skill in the art would understand that "downstream links to refer the customers' individual access links, whereas the monitor itself is placed on the physical links into the data center. Accordingly claims 1 and 11 are proper.

Regarding method claim 7, applicants have amended claim 7 to call for collecting using a provisioned monitor, statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on. Claim 7 clearly recites the subject matter of Applicant's invention. Claim 7 clearly recites that a provisioned monitor collects statistical information sent between a network to a plurality of customers of the data center by examining traffic on selected links in the data center, but collecting is performed as if the device was on downstream links.

Applicants contend that claims 24 and 29 are proper. Claim 24, for example, calls for collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs. Claim 24 is clear in that it requires collecting information on links for customers that are on downstream links.

Applicants have amended claims 12-15, 16 and 17 to provide antecedent basis for gateway. Applicants have amended the claim dependencies of claims 14 and 16 to depend from claim 13, which provides antecedent basis for global packet log. Applicants have amended claim 22 to provide antecedent basis for hosting provider ... .

The examiner rejected Claims 1-34 under 35 U.S.C. 102(e), as being anticipated by Porras et al., U.S. Patent 6,321,338.

The examiner stated in regards to claim 1 that:

> **With regards to claim 1, Porras teaches a device that collects statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on (Porras, column 3 lines 31-42, Figure 1).**

Claim 1 is distinct over Porras. Porras fails to describe or suggest a device, placed on selected links in the data center ... and that collects statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to. Rather, Porras discloses:

> **Service monitors 16a-16c provide local real-time analysis of network packets (e.g., TCP/IP packets) handled by a network entity 14a-14c. Network entities include gateways, routers, firewalls, or proxy servers. A network entity may also be part of a virtual private network. A virtual private network (VPN) is constructed by using public wires to connect nodes. For example, a network could use the Internet as the medium for transporting data and use encryption and other security mechanisms to ensure that only authorized users access the network and that the data cannot be intercepted. A monitor 16a-16f can analyze packets both before and after decryption by a node of the virtual private network.**

Porras describes a hierarchical arrangement of monitors and a VPN (virtual private network). However, nowhere does Porras disclose a device... disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets sent between the network and the data center ... for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

Claim 2 is further distinct over Porras since Porras fails to disclose that the monitoring device is coupled to a control center through a dedicated, private network. Porras fails to suggest a control center and the teachings at Col. 10, lines 27-62 fail to suggest, much less described a dedicated, private network.

Claim 3 is further distinct since Porras fails to teach a communication process that communicates statistics with the control center, and which receives queries or instructions from the control center.

Claim 4 is distinct since Porras fails to teach that the monitoring device is a gateway device and includes a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

Claim 11 is allowable over Porras since Porras fails to teach ... a provisioned monitor, placed on selected links in the data center ..., and that collects statistical information for a plurality of provisioned customers, which are on links that are downstream from the selected links ... the provisioned monitor maintaining separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

Porras fails to teach the provisioned monitor placed on selected links in the data center to collect statistical information for provisioned customers on links that are downstream from links that the provisioned monitor is disposed on. Porras also fails to teach that the provisioned monitor maintains separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link ... .

The examiner equates the event records of Porras with the counter logs. Applicants contend that this is incorrect. The event records taught by Porras, while not corresponding to the claimed counter logs are not describe or suggested as being maintained as separate counter logs for each provisioned customer. Porras also fails to suggest a global counter log that accounts for all traffic seen on the link. Claims 12-23 add additional distinct features.

Claim 7 distinguishes over Porras by calling for collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on ... .

Claim 7 is allowable for analogous reasons as in claims 1 and 11. Claims 8-10 provide additionally distinct features.

Claim 24 is allowable since Porras fails to suggest much less describe ... collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs and maintaining separate counter logs for each provisioned customer; and a global counter log that accounts for all traffic seen on the links on which collecting occurs. Claims 25-28 are allowable with claim 24.

Claim 29 is allowable with claim 7 and since it includes the additional feature of ... performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic and communicating alerts that arise from the traffic analysis.

Claims 30-34 are allowable with claim 29.

Enclosed is a **$510** check for the Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 2/9/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906